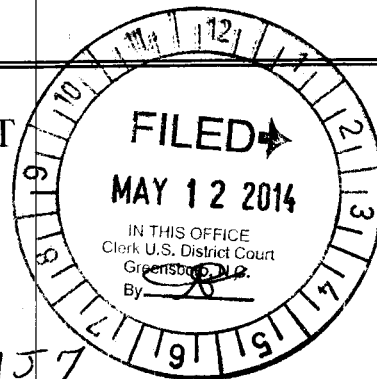


## UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina



In the Matter of the Search of  
*(Briefly describe the property to be searched  
 or identify the person by name and address)*

Peter Millar LLC  
 4300 Emperor Blvd., Suite 100  
 Durham, North Carolina

Case No. 1:14-mj-7

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Middle District of North Carolina  
*(identify the person or describe the property to be searched and give its location):*

Peter Millar LLC, located at 4300 Emperor Blvd., Suite 100, in Durham, North Carolina, and more fully described in Attachment A hereto.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized):*

See Attachment B hereto.

**YOU ARE COMMANDED** to execute this warrant on or before February 5, 2014 *(not to exceed 14 days)*  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Hon. Joi Elizabeth Peake  
*(United States Magistrate Judge)*

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for        days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of       

Date and time issued:

1/24/14 12:12 pm

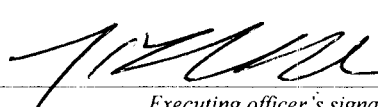
Judge's signature

City and state:

Winston Salem, North Carolina

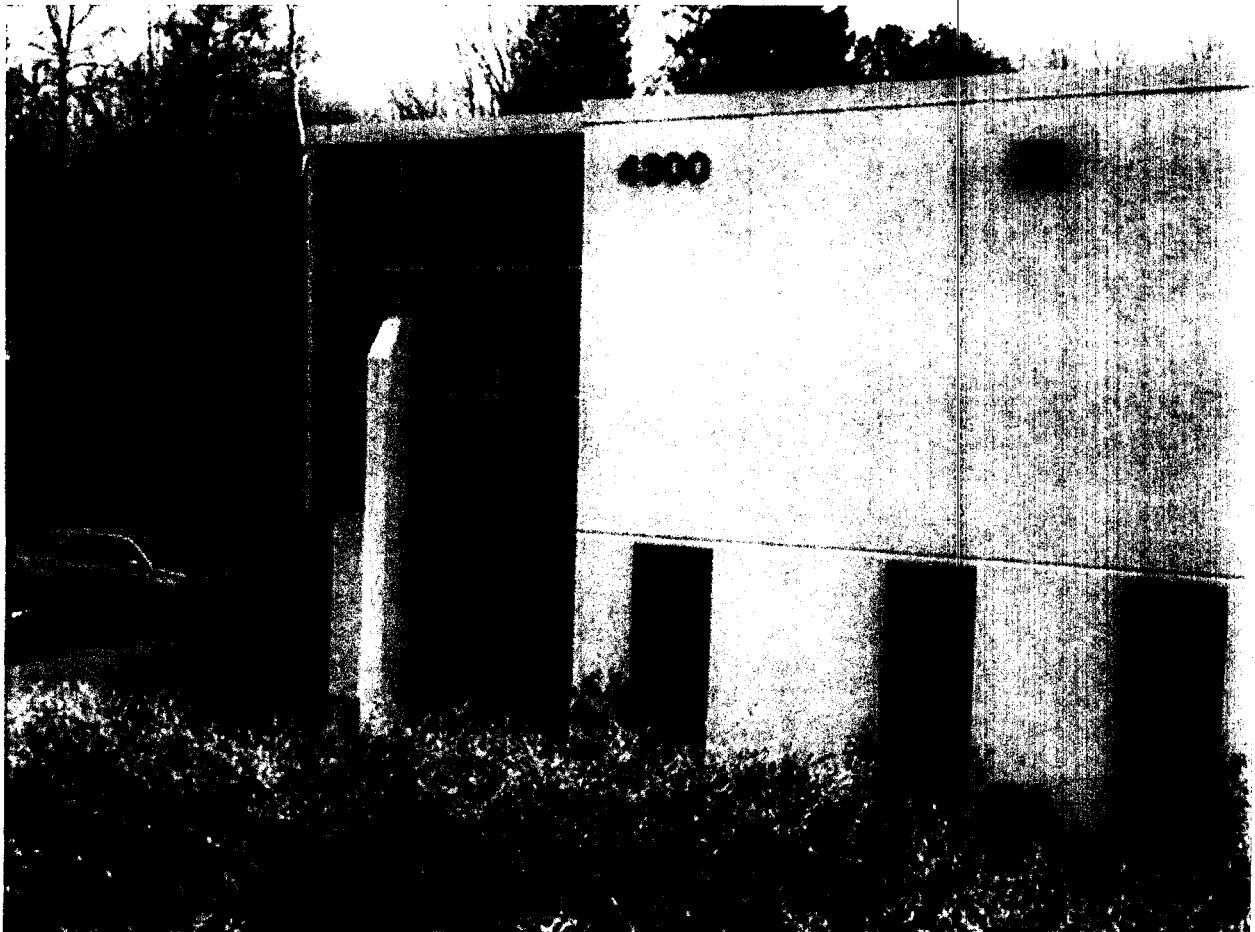
Joi Elizabeth Peake, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed: <u>1/27/14 0900</u>	Copy of warrant and inventory left with: <u>KIM MATTOON</u>
Inventory made in the presence of: <u>KIM MATTOON</u>		
Inventory of the property taken and name of any person(s) seized:		
<p style="margin-left: 40px;">9 Boxes of ENTRY DOCUMENTS</p> <p style="margin-left: 40px;">10 Boxes of JOURNAL ENTRIES</p> <p style="margin-left: 40px;">3 Boxes of FINANCIAL BINDERS / STATEMENTS</p> <p style="margin-left: 40px;">4 Boxes of AUDIT MATERIALS (2009)</p> <p style="margin-left: 40px;">14 Boxes of VENDOR WIRE / CHECKS / AP</p> <p style="margin-left: 40px;">1 BGA of MONTHLY VENDOR WIRE SUMMARIES</p> <p style="margin-left: 40px;">COPY of BLUE CHERRY DATABASE</p> <p style="margin-left: 40px;">COPY of OUTLOOK .PST. FILE</p>		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: <u>5/12/2014</u>	 <small>Executing officer's signature</small> <u>JAMES MALLOY / SPECIAL AGENT</u> <small>Printed name and title</small>	

Attachment A

The premises are located at 4300 Emperor Blvd., Suite 100, in the city of Durham, County of Durham, North Carolina, and are further described as a white office building with attached warehouse. The number "4300" is displayed on the side of the building, and the number 4300-100 is printed on the entry door to the building. Signage inside the windows of the office building denote the offices belonging to Peter Millar LLC.



### Attachment B

The items to be seized are evidence and instrumentalities of violations of Title 18, United States Code, Section 541 - entry of goods falsely classified - and Section 542 - entry of goods by means of false statements - by Peter Millar LLC from the period of April 9, 2009 to September 30, 2013, as follows:

1. Importation documentation including CBP forms filed with the United States, purchase orders, invoices, bills of lading, packing lists, and other documentation regarding the entry of foreign goods into the United States from April 9, 2009, to September 30, 2013.

2. Any documents, including electronic documents, such as bank account statements, professional or personal correspondence - including electronic mail or e-mail - from any entity, organization, or individual that would further identify importations into the United States by the company, the value of goods imported, the value of goods sold, and the identity of overseas vendors;

3. Any notices from CBP regarding importations of goods or from foreign governmental agencies regarding exportations, duties and tariffs on goods.

## Attachment C

### Computer Search Warrant Protocol

1. This search warrant covers and controls the procedure for searching: (1) electronic or computer devices, related equipment or media located at the premises set out in Attachment A to locate and seize items listed on Attachment B ("Computers"). To the extent set out in Paragraph 3 below, agents are authorized to seize and remove from the premises such Computers, including computer system input/output (I/O) peripheral devices, software and media, so that a qualified computer expert can accurately search for and retrieve the data in a laboratory or other controlled environment when this is necessary. Agents and computer experts working with agents are authorized to seize the relevant system software (operating systems, interfaces and hardware drivers), any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices (including but not limited to passwords, keycards and dongles) in order to facilitate the authorized search. In addition, if necessary for data retrieval, they are authorized to reconfigure the system in order to accurately search for and retrieve the evidence stored therein.

2. In regard to the search and inspection of Computers, agents are directed to analyze the electronically stored data, whether on-site or off-site in a laboratory or other controlled environment, by using techniques which serve to keep the search within the authorization of this warrant, such as: (a) surveying various file "directories" and the individual files they contain in order to locate evidence and instrumentalities authorized for

seizure by the warrant; (b) "opening" or reading the first few "pages" of such files or images in such files in order to determine their precise contents; (c) "scanning" storage areas to discover and possibly recover recently deleted data, and "scanning" storage areas for deliberately hidden files; and (d) performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

3. This warrant specifically requires an on-site search, or to the extent an on-site search is impractical or unreasonable, then the creation of a "mirror image" or "image" of a device, drive or media for use in an off-site search, unless such "mirror-imaging" is unreasonable under the circumstances. In general, imaging is the taking of a complete electronic picture of the devices or media, including all hidden sectors and deleted files, to obtain an exact copy of the device, drive or media's stored data without actually seizing the device, drive or media. The agent or an expert will then conduct an off-site search for information or data described in the warrant from the "mirror image" copy at a later date. In the event that mirror-imaging reasonably cannot be done under the circumstances, or cannot reasonably be done on-site under the circumstances, agents are authorized to seize and remove from the premises such electronic or computer devices but must return them to the subject premises within seven days of removal, absent further permission from the court.

4. Searching electronic or computer devices for criminal evidence can be a highly technical process requiring expert skill and a properly controlled environment. The vast array of

electronic and computer hardware and software extant may require a computer expert who specializes in specific systems and applications, all of which may be impossible to ascertain before the search. Moreover, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected or encrypted files. Because electronic and computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Consequently, to the extent set out in Paragraph 3, this warrant authorizes the temporary seizure of electronic or computer devices and their input/output peripheral devices, related software, documentation, data security devices (including passwords) and media so that a qualified computer expert can accurately retrieve the data in a laboratory or other controlled environment.

5. When an electronic or computer device, hardware, equipment, software or media has been seized for off-site search and analysis, the agents shall comply with Fed. R. Crim. P. 41(f) in the following manner. Following the initial search and seizure, the agents shall prepare the usual Rule 41(f) inventory of not only the property and items seized by them pursuant to the warrant, but also the information or data, which has, at that date, been identified as "seized" pursuant to the warrant. This inventory will identify each electronic or computer device, related equipment or media, which will be subject to further off-site, search for additional information. For example, if the agents make an on-site mirror image of a drive, device or media, for use in an off-site search, they need only list the

making of the mirror image in the return, with an indication that it is subject to further searching pursuant to this warrant. The listing of any data or information, which is "seized" from the media off-site, will then be made in the final inventory return. The agents shall give or leave a copy of the warrant and receipt of this preliminary inventory of property seized and make a return to the court, all as provided by Rule 41(f).

6. After completing the initial search and seizure and preparing the inventory, the agents are directed to immediately begin the off-site search and information retrieval process with respect to the electronic or computer devices, related equipment and media which have been seized and on which further data retrieval is continuing. The agents shall complete the search and data retrieval process within thirty days of the execution of this warrant (unless an extension of time is obtained by the government) and, at that time, prepare a final inventory of information or data seized by them during the off-site search and both deliver a copy of the final inventory of information or data seized by them during the off-site search to the person from whom or from whose premises the property was taken (if known) and make a return of the original final inventory to the court. The court will then attach this final inventory to the original search warrant and inventory return as an addendum. Because of the nature of electronic or computer information, the listing of "seized data" in the inventory return may be made by copying the "seized data" to a computer diskette or CD or DVD disc and submitting it, along with an affidavit which explains what is on the diskette or disc and the procedure used.



7. If the owner of the seized items so requests, pursuant to Fed. R. Crim. P.41(g) the agents will, to the extent practicable, attempt to provide such owner with copies of any files, data or information, that may be necessary or important to such owner's legitimate activities. The items seized are subject to the time limit and other terms for the return of seized property set forth above.

## Attachment D

### Protocol for Potentially Privileged Materials

1. Prior to the execution of the search, the United States Attorney's Office for the Middle District of North Carolina shall identify one Assistant United States Attorney to be a member of the taint team. Similarly, Homeland Security Investigations shall designate two agents to be members of the taint team: one investigative agent and one forensic examiner.

2. The members of the taint team shall have no prior involvement in the investigation and will have no further role in the investigation or prosecution of this case after review of the subject items, unless some further privilege issue arises requiring additional review or litigation. Everyone participating in the taint team review of the subject items shall review and be familiar with these procedures.

3. The taint team shall obtain from the prosecution team sufficient factual information about the nature and scope of the criminal investigation so that the taint team can conduct its review in a complete, thorough and professional manner. The taint team shall be responsible for the secure storage of all privileged information. The material shall be stored in a facility segregated from the other documents and tangible objects gathered as part of the underlying investigation. Access to the privileged information shall be limited to the members of the taint team. The taint team shall create and maintain a log showing the names of the members of the taint team and the dates and times when those members obtained access to the privileged information for review.

4. If it is anticipated that privileged information will be obtained during the course of a search, the taint team shall be present at the search location, if practicable. However, the

attorney members of the taint team shall not participate in the search itself. The agent members of the taint team shall participate in the search and take possession of the privileged information and shall conduct a preliminary review to determine whether the information is truly privileged, whether the privileged information falls within the scope of the search's lawful parameters, whether the privileged information is relevant to the investigation, and whether the privileged information is subject to some exception which would overcome the privilege.

5. The attorney member of the taint team shall provide legal advice and guidance to the agent and may participate in the review of the materials.

6. The taint team shall not disclose any of the privileged information to the prosecution team. Nor shall the taint team discuss its preliminary findings with respect to the information reviewed with the prosecution team.

7. Once the taint team has completed its preliminary review, any materials which the taint team determines clearly not to contain privileged information may be given to the prosecution team. Any materials which the taint team determines clearly to be privileged information for which there is no exception which would overcome the privilege, or is irrelevant, or is outside the scope of the lawful parameters of the search, shall be returned to the owner. The taint team shall not make or retain any copies of such privileged information. Any materials which the taint team determines to arguably contain privileged information or arguably to be subject to an exception to the privilege shall be submitted to the Court for a final determination of privilege.